

ABSTRAK

Fahru Roszy Mahtuf. K3513075. **PENGEMBANGAN LABORATORIUM VIRTUAL UNTUK SIMULASI UJI PENETRASI KEAMANAN JARINGAN**. Skripsi, Surakarta: Fakultas Keguruan dan Ilmu Pendidikan Universitas Sebelas Maret Surakarta, Oktober 2018.

Penelitian ini bertujuan untuk mengembangkan sebuah server yang terisolir menggunakan teknik virtualisasi untuk simulasi uji penetrasi.

Metode penelitian yang digunakan dalam penelitian ini adalah Research and Development dengan menerapkan model pengembangan Network Development Life Cycle (NDLC) dari Goldman & Rawles yang telah dimodifikasi. Tahap-tahap pengembangan terdiri dari 1) Analisis. 2) Desain. 3) Implementasi. 4) Pengujian.

Hasil dari penelitian ini adalah Penetration Testing dapat dilakukan pada lingkungan server yang bersifat terisolir atau bersifat virtual. Hasil pengujian performa menunjukkan server virtual mampu memaksimalkan penggunaan resource memory sebesar 80% dibandingkan penggunaan resource memory server fisik sebesar 35%. Pengujian penggunaan CPU pada kedua server menunjukkan hasil yang baik yaitu penggunaan resource CPU tidak lebih dari 50%. Berbanding terbalik dengan pengujian performa Response Time dan Throughput, server fisik memiliki keunggulan yang jauh dari server virtual. Response Time server fisik rata-rata sebesar 54.917 duration/sec dan server virtual nilai rata-rata Response Time sebesar 55.349 duration/sec. Nilai Throughput server fisik memiliki kecepatan transfer 10 kali lebih cepat dibandingkan server virtual. Berdasarkan hasil pengujian keseluruhan server fisik lebih baik dibandingkan server virtual, tetapi virtual server memiliki keunggulan dalam memanfaatkan penggunaan resource dibandingkan dengan server fisik

Kata kunci : *Server Virtual*, Virtualisasi, Uji Penetrasi.

ABSTRACT

Fahru Roszy Mahtuf K3513075. VIRTUAL LABORATORY DEVELOPMENT FOR SIMULATION OF NETWORK SECURITY PENETRATION TEST. Thesis, Surakarta: Faculty of Teacher Training and Education Sebelas Maret University Surakarta, October 2018.

This study aims to develop a server that is isolated using virtualization techniques for simulation of penetration tests.

The research method used in this study is Research and Development by applying the modified Network Development Life Cycle (NDLC) development model from Goldman & Rawles. The development stages consist of 1) Analysis. 2) Design. 3) Implementation. 4) Testing.

The results of this study are Penetration Testing can be done on a server environment that is isolated or virtual. Performance testing results show that virtual servers can maximize memory resource usage by 80% compared to physical server memory resource usage by 35%. Testing of CPU usage on both servers shows good results, ie CPU resource usage is not more than 50%. Inversely with testing the performance of Response Time and Throughput, physical servers have advantages that are far from virtual servers. The physical response time server averaged 54,917 duration / sec and the virtual server average response time was 55,349 duration / sec. The value of physical server throughput has a transfer rate 10 times faster than a virtual server. Based on the results of testing the entire physical server is better than virtual servers, but virtual servers have the advantage of utilizing resource usage compared to physical servers

Keywords: Virtual Server, Virtualization, Penetration Testing